NRCS
Natural Resources Conservation Service
Wallace F. Bennett Federal Building
125 South State Street, Room 4402
Salt Lake City, UT 84138-1100

September 19, 2008

UTAH BULLETIN UT130-08-01

SUBJECT: PROCEDURES FOR SAFEGUARDING PERSONALLY IDENTIFIABLE INFORMATION AND OTHER SENSITIVE INFORMATION.

Expiration Date: Until further notice.

Purpose: To create a procedure in Utah for storing, sending, or transmitting Personally Identifiable Information (PII) and any other sensitive information.

Personally Identifiable Information is information that can be used to distinguish or trace identity. Examples include social security numbers or medical records, or information that, when combined or used with other identifying information, is linked or linkable to a specific individual.

Employee Responsibility

- Every employee who has access to personally identifiable information of other employees, contractors, or the general public through the course of his or her employment at USDA is required to safeguard and protect such information from unauthorized disclosure.

- Every employee is required to immediately report any known or suspected breach of the PII safeguards or policies, or actual unauthorized disclosure of PII to his or her supervisor.

When PII or other sensitive information is stored, sent, or transmitted NRCS Utah employees must follow the following procedures.

➢ STORING PII AND OTHER SENSITIVE INFORMATION

- Storing of PII and other sensitive information will be done in locations that are locked or password protected. This information will only be accessible to those employees who "need to know" the information in order to conduct job duties.

- Hard copy storing of PII and other sensitive information will be done in a locked location (i.e. locked desk, locked file cabinet, and/or locked fire proof safe).

- Electronic devices with PII and other sensitive information, when not in use, must be locked up (i.e. laptops, hard drives, cell phones, PDAs and Blackberries).

- Electronic storing of PII and other sensitive information will be done in password protected locations where only those employees that need the information have the password (i.e. H: drive). Storing PII information on the C: drive of your computer for example would not meet this requirement. If PII and other sensitive information needs to be stored electronically (i.e. C: drive), Utah NRCS employees will follow these steps:

    - Using WinZip the file will be encrypted using 256-Bit AES Encryption.
    - Password for this encryption will only be known to the employees needing access to the information. The password that NRCS Utah will use for this will be different in every office throughout the state and will be distributed on a "need to know" basis. **This password must not be written down, emailed, or recorded.**
    - After encryption the file will be zipped for storage.

See Attachment A "SOP Title: Encryption and Password Protection To Safeguard Sensitive and Private Information" for specific guidance on how to encrypt a file using WinZip. For saving files, follow the steps to 4.3.12 and then delete the unencrypted file. After deletion empty the computers recycle bin.

Note: First time users of WinZip will need to click on "send to" then "Compressed (zipped) Folder" and then "open with" see Attachment B.

➢ SENDING OR TRANSMITTING PII OR OTHER SENSITIVE INFORMATION

If PII or other sensitive information needs to be sent or transmitted the following procedures must be followed.

- **Fax** – Faxing is considered a secure means to transmit information. If PII is transmitted by fax an employee should notify the person that will receive the fax that they are sending the information. Once sent the person receiving the PII will wait for it at the fax to prevent unwanted viewing of the information.

- **Land Line Phone** – Land line phones are considered a secure means to transmit information. Make sure that the person you are speaking to "needs to know" and is authorized to have the information requested.

- **Cell Phones** – Cell phones are not considered a secure means to transmit information and will not be used to transmit any PII information. This includes both voice and/or text messaging.

- **Ground Mail** – Ground mail is considered a secure means to transmit PII information. Steps should be taken to make sure information is not visible through the envelope. Also steps will be taken to insure the envelope will only be opened by the intended recipient.

- **E-mail** – E-mail is not considered a secure means to transmit information. PII information will not be emailed unless the following steps are taken.

    - With WinZip the file will be encrypted using 256-Bit AES Encryption.
    - The password for this encryption will only be known to the employees needing access to the information. After emailing the attachment the password should be sent in a separate email. The password can be user chosen.
    - After encryption the file can then be emailed.

See attachment A "SOP Title: Encryption and Password Protection To Safeguard Sensitive and Private Information" for specific guidance on how to encrypt and then email a file using WinZip.

Note: First time users of WinZip will need to click on "send to" then "Compressed (zipped) Folder" and then "open with" see attachment B.

Contacts:
Lisa Rice, State FOIA/Privacy Act Officer - (801) 524-4587 Lisa.Rice@ut.usda.gov
James Huggard, State Technology Coordinator - (801) 524-4587 James.Huggard@ut.usda.gov

/S/

SYLVIA A. GILLEN
State Conservationist

Attachments

Distribution: E